REMARKS

The specification has been amended. Claims 1, 4, 6 - 13, 18 - 19, 21 - 22, 25, 27 - 34, 39 - 40, and 42 - 46 have been amended. Claims 47 - 48 have been added. No new matter has been introduced with these amendments or added claims, which are supported in the specification as originally filed. Claims 2 - 3, 5, 14 - 17, 23 - 24, 26, and 35 - 38 have been cancelled from the application without prejudice. Claims 1, 4, 6 - 13, 18 - 22, 25, 27 - 34, and 39 - 48 are now in the application.

I. Rejection Under 35 U.S.C. §103(a)

Paragraph 3 of the Office Action dated January 27, 2005 (hereinafter, "the Office Action") states that Claims 1 - 17, 19 - 38, and 40 - 46 are rejected under 35 U.S.C. §103(a) as being unpatentable over U. S. Patent 5,862,323 to Blakley et al. in view of U. S. Patent 6,615,258 to Barry et al. Paragraph 4 of the Office Action states that Claims 18 and 39 are rejected under 35 U.S.C. §103(a) as being unpatentable over Blakley in view of Barry and further in view of U. S. Patent 6,240,184 to Huynh et al. Claims 2 - 3, 5, 14 - 17, 23 - 24, 26, and 35 - 38 have been cancelled from the application without prejudice, rendering the rejections moot as to those claims. The rejections are respectfully traversed with regard to remaining Claims 1, 4, 6 - 13, 18 - 22, 25, 27 - 34, and 39 - 46.

Applicants have amended their independent Claims 1, 22, and 43 herein to more clearly specify that a password synchronization agent, or "PSA", receives "a password propagation request providing an identifier of the user [from whom the request is received] and an identifying

secret of the user" (Claim 1, lines 10 - 11, emphasis added). Blakley fails to teach this limitation, and thus fails to teach responsive limitations (i.e., "forwarding ... the received user identifier and identifying secret ...", etc.) as specified in Applicants' independent claims.

By contrast, Blakley teaches (in a first of two approaches) a propagation request processing technique that is initiated from a "foreign registry". Blakley refers to this technique as a"pull" technique, and Blakley's Fig. 4 illustrates this technique. As shown therein, the processing begins at **Block 424**, where a foreign registry "Z" requests a copy of client "W"'s password. Following this flow through to **Block 448**, Blakley's password synchronization server "retrieves client W's [password] from the [password] repository and decrypts it" (emphasis added). This decrypted password is then returned to foreign registry Z in **Block 452**. Notably, the password repository (shown as element **112** in **Fig. 3B**) stores passwords in recoverable form -- that is, a form from which the decrypted version can be recovered. See col. 8, lines 40 - 44, which discuss the operations of **Blocks 448** and **452** (misstated in line 43 as **Block 450**). See also col. 11, lines 38 - 41, stating

> "... the password synchronization server supports plain-text password retrieval by a foreign registry upon foreign registry request. This operation is also called "password synchronization pull." (emphasis added)

Furthermore, col. 16, lines 26 - 27 specify "Foreign registries will "pull" a recoverable plain-text password when needed ..." (emphasis added). See also col. 11, lines 59 - 60, "... the password synchronization server recovers plaintext passwords from disk storage" (emphasis added).

This is distinct from Applicants' claimed technique, which specifies a trusted authenticating domain that "... stores identifying secrets for user identifiers only as secured, non-recoverable versions thereof" (see lines 15 - 17 of Claim 1, emphasis added).

It is to be further noted that the target of the propagation, when using Blakley's "pull" technique, is the same foreign registry from which the request was received. And, Blakley's pull technique propagates information recovered from the password synchronization server (col. 11, lines 59 - 60). By contrast, Applicants' claim limitations specify receiving the propagation request from a client device (Claim 1, line 8) and then propagating information provided therein to a master registry (Claim 1, lines 23 - 25).

In summary, receiving a request from a foreign registry, and retrieving and decrypting a password for propagating to that requesting foreign registry, as taught by Blakley for his pull technique, is patentably distinct from Applicants' claimed technique by virtue of (at least) the following limitations:

- "... receiving, ... from a user at a client device ..., a password propagation request providing an identifier of the user and an identifying secret of the user" (Claim 1, lines 7 - 11, emphasis added);
- "... wherein the trusted authenticating domain stores identifying secrets for user identifiers only as secured, non-recoverable versions thereof" (Claim 1, lines 15 - 17, emphasis added); and
- "... propagating ... the received user identifier and identifying secret ... to a master

registry ..." (Claim 1, lines 23 - 29, emphasis added).

Thus, it can be seen that Applicants' claimed invention is patentably distinct from Blakley's "pull" technique.

In a second approach, Blakley specifies a "push" technique. However, Blakley 's disclosed "push" technique (which is illustrated in **Figs. 3C** and **5**) operates responsive to a user requesting to initially set or update his/her password. See, for example, the text in **Block 510**, where the processing flow of **Fig. 5** begins, stating "Client Y requests account creation or password change ..." (emphasis added). See also col. 8, lines 45 - 48, stating "... automatically propagate password changes for selected users (accounts) to one or more foreign registries requiring this data" (emphasis added) and lines 57 - 59, stating "... the client of Y first requests account creation or a password change ..." (emphasis added).

This "push" approach is also distinct from Applicants' claimed invention. In particular, since Blakley's "client Y" has now provided a new or different password for this the password push technique, the processing that is performed to determine whether this new/different password can be propagated involves checking attributes of potential targets and a password propagate flag ("PW_PROPAGATE_ENABLE"), but notably, does not involve a trusted authenticating domain creating a validation result that indicates whether the trusted authenticating domain itself "had previously stored, for the user identifier, a secured version of the identifying secret" (see Applicants' Claim 1, lines 19 - 22, emphasis added) that was

provided on a request received from a user (Claim 1, lines 10 - 11).

As demonstrated above, Applicants respectfully submit that their independent Claims 1, 22, and 43 contain a number of limitations not taught by Blakley. Barry also fails to teach these limitations: the cited text from Blakley simply refers to validating a user's password and counting the number of retry attempts that are allowed before concluding that the user's password cannot be successfully validated. Huynh also fails to teach the limitations discussed above. Independent Claims 1, 22, and 43 are therefore deemed patentable over the references. Dependent Claims 4, 6 - 13, 18 - 21, 25, 27 - 34, 39 - 42, and 44 - 46 are therefore deemed patentable over the references as well. Accordingly, Applicants respectfully request that the Examiner withdraw the §103 rejection.

II. Conclusion

Applicants respectfully request reconsideration of the pending rejected claims, withdrawal of all presently outstanding rejections, and allowance of all remaining claims at an early date.

Respectfully submitted,

Marcia L. Doubet

Marcia L. Doubet
Attorney for Applicants
Reg. No. 40,999

Customer Number for Correspondence: 43168
Phone: 407-343-7586
Fax: 407-343-7587